



EXECUTIVE BRIEFING 02 / SEPTEMBER 2026

Connected work. Governed operations.

The business operating system inside DeskBridge
Workspace.

DESKBRIDGE SOVEREIGN • AT A GLANCE

- 01 Shared records across business functions
- 02 Access shaped by role, company and purpose
- 03 Essentials, Business and Control capability

Secure workspaces. Managed access. Audit ready.
deskbridge.uk/briefings/sovereign/

The operating model

Most business software gives you separate screens. DeskBridge Sovereign brings records, people, documents and day-to-day work together, with clear controls and evidence of what happened.

DeskBridge Sovereign is the application family inside DeskBridge Workspace. It connects records, people, documents, communication, work and operational insight through one access and evidence model. Every DeskBridge Workspace includes Sovereign; the package determines the depth of applications, managed operation and assurance around it.

What Sovereign is designed to solve

Organisations often run core work through separate systems that do not share a consistent authority model. Customer information sits in one place, people data in another, documents in a third, tasks in email, and operational decisions in spreadsheets. The result is duplicated data, inconsistent permissions and a trail of evidence that has to be reconstructed.

Sovereign is built around clear product boundaries and shared contracts. Core records, identity, parties, products, currencies, workflows, documents, messages, events and immutable audit are treated as governed foundations. Specialist applications consume only the information they need for their purpose, with tenant, company, role and record scope enforced in the API rather than merely hidden in a menu.

The Sovereign application family

Directory, Flow and Vault: the Essentials foundation

Directory provides the governed people, organisation and relationship foundation. Flow supports operational processes such as orders, purchasing, stock and business activity. Vault provides protected document access and, where entitled, records lifecycle functions such as retention, holds and disposal. Together they create a controlled base for everyday work.

Claim

Claim supports expenses and spend claims, connecting them to the right people, documents and accounting dimensions without exposing the full financial workbench to every user.

People

People manages employee and employment authority, including joiner, mover and leaver workflows, employment documents and purpose-limited projections to authorised consumers.

Engage

Engage supports customer engagement, marketing and service activity using canonical parties and governed product information, so client-facing work does not create another uncontrolled customer master.

Connect

Connect governs messages, delivery channels, routing, providers and integration operations. It gives communication an operational identity and evidence trail rather than leaving critical decisions in disconnected mailboxes.

WorkHub

WorkHub brings work, collaboration and delivery activity into the governed workspace, so teams can coordinate without automatically creating new unowned data stores and sharing paths.

Insight

Insight provides operational visibility. The aim is not another dashboard for its own sake, but a clearer view of what is happening, what needs attention and what evidence management can rely upon.

Ledger and Forge

The Control tier adds Ledger for books, journals, tax, reconciliation and financial workbenches, and Forge for manufacturing definitions and execution. Advanced Insight and control reporting complete the stronger assurance and management layer.

Security, DBAV and Guardian

Sovereign is not just a collection of modules. Its value comes from the way access and evidence follow the work. Permissions are separated from product entitlement. Cross-product changes use versioned contracts, correlation identifiers and idempotency. Audit evidence is immutable and linked to the action, not written as an afterthought.

DBAV protects the content boundary. It combines established malware scanning with bounded analysis of files and documents for suspicious structures and behaviour indicators. It can detect risky macros, scripts, web-shell patterns, credential-theft indicators and ransomware-related file-integrity signals, while keeping verdict records metadata-only. A finding can stop automated release until an authorised review takes place.

Guardian turns that signal into governed operational protection. It independently checks the precise target, tenant and approvals before a containment action is allowed. It can preserve evidence and rollback references and support controlled freeze, isolation or recovery workflows. Guardian does not blindly obey a scanner, and DBAV never executes a destructive response. This separation gives the organisation a defensible chain from detection to decision to authorised action.

The result is security that is explainable: what happened, which policy applied, what was affected, who approved the response, what was preserved, and how the organisation returned to a known state.

Where Sovereign can reduce cost

Disconnected applications create a tax that rarely appears on a software invoice. Teams re-key data. Administrators reconcile conflicting records. Managers chase approvals. Support teams explain which system is authoritative. Auditors ask for evidence that exists in fragments. Integrations become one-off dependencies that nobody wants to own.

Sovereign reduces that cost by making the operating model coherent. One governed identity and access model can serve multiple business functions. Shared contracts reduce duplicate masters. Purpose-limited access reduces over-provisioning. Common support and evidence patterns reduce the cost of proving and maintaining control.

For a smaller organisation, that means enterprise discipline without building every application, integration and control internally. For a larger or regulated organisation, it means a more deliberate authority model and a clearer path to evidence-backed assurance.

Built for real operating boundaries

Sovereign is designed to work with the client rather than demand that every existing dependency disappears overnight. DeskBridge can operate alongside Microsoft 365 where necessary, add governance around existing environments, and scope mail, integrations, contractor access, AI governance and assurance according to the client's requirements.

This is the difference between buying a group of applications and adopting a managed operating model. Sovereign connects the work. Workspace protects the working environment. DeskBridge support and evidence make the whole service accountable.

DeskBridge Sovereign: connected operations, governed access and evidence you can use.

What a business can actually run in Sovereign

DeskBridge Sovereign is not simply an accounts package, an ERP or an M-ERP. It is the connected business operating layer inside DeskBridge Workspace, combining the tools an organisation needs to run its business: customer and supplier records, sales, purchasing, invoicing, finance workflows, expenses, people operations, payroll-ready HR processes, stock, production, projects, documents, communications, reporting and evidence.

A client can use Sovereign to maintain customers and suppliers, quote and sell work, raise invoices, purchase materials, receive and issue stock, manage warehouses, plan production, track batches or serials, run projects, control documentation, submit and approve expenses, manage employees and payroll-ready information, coordinate communications, review management information and retain the evidence behind important actions.

That makes Sovereign relevant to businesses of any size. A small company can begin with the functions it needs now and expand its operating model as it grows. A larger organisation can connect departments, projects, contractors and suppliers without giving every user access to every system. Existing specialist finance or sector systems can remain where appropriate while DeskBridge governs access, support, migration and evidence around them.

Start with the outcome your organisation needs.

Tell us your team size, the systems you use today and the access, workflow or evidence problem you most want to solve.

01 • Workspace

The controlled working environment.

02 • Sovereign

The connected business applications.

03 • Pilot

A scoped, supported evaluation.

Request a pilot scope review

deskbridge.uk/briefings/pilot/

£12 per user per month for the first three months. Sign up by 30 October 2026. Acceptance, application readiness and agreed service scope apply.

Read the companion briefings

[DeskBridge Workspace](#) — See how named access, onboarding, offboarding, support and security evidence fit into one managed working environment.

[DeskBridge Pilot Programme](#) — Review the £12 per user per month paid pilot, first-three-month offer, migration and hosting benefits, scope and application process.

Contact DeskBridge

deskbridge.uk/contact/
contact@deskbridge.uk

Capabilities depend on the agreed package, deployment and readiness. This briefing describes the service model; your written proposal defines the delivery scope. Pilot migration charges, hosting requirements, tax treatment and post-pilot pricing are confirmed in the quote.

DeskBridge Ltd · Company number 17123038 · Wales, United Kingdom
Edition 1.0 · 7 September 2026